IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Massimiliano Antonio Poletto et al.	Art Unit	: 2135
Serial No.	: 09/931,344	Examiner	: Ha, L.
Filed	: August 16, 2001	Conf. No.	: 2635
Title	: DEVICE TO PROTECT VICTIM SITES DURING DENIAL OF SERVICE ATTACKS		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF ON BEHALF OF MASSIMILIANO ANTONIO POLETTO ET AL

The Appeal Brief fee has already been paid. If an additional fee is due, please apply that fee and any other charges or credits to Deposit Account No. 06-1050.

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: October 24, 2007

(i.) Real Party In Interest

The real party in interest in the above application is Mazu Networks, Inc.

(ii.) Related Appeals and Interferences

The appellant is not aware of any appeals or interferences related to the above-identified patent application.

(iii.) Status of Claims

This is an appeal from the decision of the Primary Examiner in an Office Action dated April 18, 2006, rejecting claims 1-39, all of the claims in the application. Claims 1-39 are the subject of this appeal.

(iv.) Status of Amendments

Appellant filed a Reply to the Final Office Action of April 19, 2006, amending claims 1 and 16 to correct the informalities pointed out by the examiner and to incorporate a portion of the preamble into the body of those claims.

In an advisory action dated July 20, 2006, the examiner did not enter the amendment indicating that amendments to claims 1 and 16 required further consideration and or search. Appellant elected to file a Notice of Appeal (October 19, 2006) and Appeal Brief on February 13, 2007. The claims on appeal are those that existed prior to the final action of July 20, 2006.

In response to Appellant's Appeal Brief, the examiner re-opened prosecution in an Office action dated **June 26, 2007**. Appellant has elected to re-instate the appeal and has filed a new Notice of Appeal herewith.

(v.) Summary of Claimed Subject Matter

Claim 1

One aspect of Appellant's invention is set out in claim 1 as a gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises a computing device. *"The arrangement 10 to protect the victim*

includes a control center 24 that communicates with and controls gateways 26 and data collectors 28 disposed in the network 14. The arrangement protects against DoS attacks via intelligent traffic analysis and filtering that is distributed throughout the network."[1]

Inventive features of claim 1 include a monitoring process that monitors network traffic through the gateway. "*The gateway 26 includes a monitoring process 32 (FIG. 6B) that monitors traffic that passes through the gateway ... .*"[2]

Inventive features of claim 1 also include a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center. "... *as well as a communication process 33 that can communicate statistics collected in the gateway 26 with the data center 24.*"[3]

Inventive features of claim 1 also include a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack. "*In addition, the gateway 26 can include processes 35 to allow an administrator to insert filters to filter out, i.e., discard packets that the device deems to be part of an attack, as determined by heuristics described below.*"[4]

Claim 16

Another aspect of Appellant's invention is set out in claim 16 as a method of protecting a victim site during a denial of service attack. *Appellant's originally filed claims and summary discuss a method.*

Inventive features of claim 16 include disposing a gateway device between the victim site and a network. "*Referring to FIG. 2, details of an exemplary deployment of a gateway is shown. Other deployments are possible and the details of such deployments would depend on characteristics of the site, network, cost and other considerations. The gateway 26 is a program executing on a device, e.g., a computer 27 that is disposed at the edge of the data center 20 behind an edge router at the edge of the Internet 14.*"[5]

---

[1] Appellant's specification Page 5, lines 17-22.
[2] Id. Page 7, lines 9-10.
[3] Id. Page 7, lines 10-13.
[4] Id. Page 7, lines 17-20.
[5] Id. Page 6, line 27 to Page 7, line 2.

Inventive features of claim 16 also include monitoring network traffic through the gateway and measuring heuristics of the network traffic to provide statistics network traffic. This feature finds support as the analogous feature of claim 1.

Inventive features of claim 16 also include communicating the statistics collected in the gateway to a control center. This feature finds support as the analogous feature of claim 1.

Inventive features of claim 16 also include filtering out packets that the gateway or control center deems to be part of an attack. This feature finds support as the analogous feature of claim 1.

Claim 29

Another aspect of Appellant's invention is set out in claim 29 as a computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises instructions for causing a computer device coupled at an entry to the site to. *"The gateway 26 and data collector 26 are typically software programs that are executed on devices such as computers, routers, or switches."*[6]

Inventive features of claim 29 include instructions to monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic. This feature finds support as the analogous feature of claim 1.

Inventive features of claim 16 also include instructions to communicate statistics collected in the computer device to a control center. This feature finds support as the analogous feature of claim 1.

Inventive features of claim 16 also include instructions to filter out packets that the device or control center deems to be part of an attack. This feature finds support as the analogous feature of claim 1.

(vi.) Grounds of Rejection to be Reviewed on Appeal

(1) Claims 1, 16 and 29 are provisionally rejected on the ground of non-statutory double patenting over claims 1, 9, 18 and 21 of co-pending Application No. 09/931,291.

---

[6] Id. Page 9, lines 6-9.

(2) Claims 1, 16, and 29 are provisionally rejected on the ground of non-statutory double patenting over claims 1, 3 and 4 of co-pending Application No. 10/066,252.

(3) Claims 1-39 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson (US 6,990,591), and further in view of Cheriton (US 7,120,931).

(vii.) Argument

"It is well established that the burden is on the PTO to establish a prima facie showing of obviousness, *In re Fritsch*, 972 F.2d. 1260, 23 U.S.P.Q.2d 1780 (C.C.P.A., 1972)."

In *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, (2007), the Supreme Court reversed a decision by the Court of Appeal's for the Federal Circuit decision that reversed a summary judgment of obviousness on the ground that the district court had not adequately identified a motivation to combine two prior art references. The invention was a combination of a prior art repositionable gas pedal, with prior art electronic (rather than mechanical cable) gas pedal position sensing. The Court first rejected the "rigid" teaching suggestion motivation (TSM) requirement applied by the Federal Circuit, since the Court's obviousness decisions had all advocated a "flexible" and "functional" approach that cautioned against "granting a patent based on the combination of elements found in the prior art."

With respect to the genesis of the TSM requirement, the Court noted that although "As is clear from cases such as Adams[7], a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. Although common sense directs one to look with care at a patent application that claims as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known."

[7] United States v. Adams, 383 U. S. 39, 40 (1966)

In application of the TSM requirement, the Court cautioned that: "Helpful insights, however, need not become rigid and mandatory formulas; and when it is so applied, the TSM test is incompatible with our precedents."

"The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Gordon*, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984).

> Although the Commissioner suggests that [the structure in the primary prior art reference] could readily be modified to form the [claimed] structure, "[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Laskowski*, 10 U.S.P.Q. 2d 1397, 1398 (Fed. Cir. 1989).

"The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination." *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 488 (Fed. Cir. 1984).

> Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under Section 103, teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) (emphasis in original, footnotes omitted).

"The critical inquiry is whether 'there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.'" *Fromson v. Advance Offset Plate, Inc.*, 225 U.S.P.Q. 26, 31 (Fed. Cir. 1985).

(1) Claims 1, 16 and 29 were provisionally rejected on the ground of non-statutory double patenting over claims 1, 9, 18 and 21 of co-pending Application No. 09/931,291.

Appellant will consider timely submission of a terminal disclaimer upon indication of allowable subject matter.

(2) Claims 1, 16, and 29 were provisionally rejected on the ground of non-statutory double patenting over claims 1, 3 and 4 of co-pending Application No. 10/066,252.

Appellant will consider timely submission of a terminal disclaimer upon indication of allowable subject matter.

(3) Claims 1-39 are not obvious over any combination of Pearson with Cheriton.

Claims 1, 3, 4, 14, 16, 18, 19 and 28

Claim 1

For the purposes of this appeal only, claims 1, 3, 4, 14, 15, 16, 18, 19 and 28 stand or fall together. Claim 1 is representative of this group of claims.

Claim 1 is directed to a gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, with the gateway including a computing device. Pearson taken in any combination with Cheriton, neither describes nor suggests a computing device that includes "... a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center and a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack."

The examiner contends that:

As per claim 1:

discloses gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises: a computing device comprising:

a monitoring process that monitors network traffic through the gateway; (col.6, lines 6-19; Pearson discloses a communication device 106 is also referring to a gateway, firewall, or other devices that communicates data between one or more ports. The firewall and intrusion detection functionality of communication device protects the resources of LAN from potential hackers. Thus, the claimed gateway will hereinafter refer to the communication device 106.)

a communication process that communicate statistics collected in the gateway from the monitoring process (col. 8, lines 10-15 and col. 19, lines 45-50) with a control center and that receives queries or instructions from the control center; (col.7, lines 55-62; col.9, lines 11-17; FIG.1 (controller 112);

and col.20, lines 40-50; Pearson discloses the remoter monitoring center (RMC) 130 comprises several components that provide functionality for carrying out various tasks (col. 6, lines 42-55). The RMC is the claimed control center where the communication device carries out communications from the RMC (col. 15, lines 52-65 and col. 16, lines 26-29).)

and [a filtering process to insert filters on network devices to filter out packets] that the gateway deems to be part of an attack, (col.9, lines 11-16 and col. 16, lines 36-53)

Pearson discloses a predetermined level of network security, that is, monitoring for certain predetermined responses to such threats, may be established (col. 10, lines 56-64) where the RMC is operative in response to the selection to one of the selectable security levels to automatically configure the communication device to monitor for certain predetermined threats and to provide certain predetermined responses (co. 11, lines 7-12). Further, Pearson discloses remote agents may be software application programs for classifying and handling identified security risks (col. 18, lines 21-24). Thus, Pearson suggests selectively configure to monitor certain threats and of security levels.

Pearson seems to suggest the claimed a filtering process to filter out packets by an intrusion detector and that all communications are analyzed and compared to the list of known attacks (col.9, lines 11-16 and col. 16, lines 36-53).

However, Pearson did not particularly discusses a filtering process to insert filters on network devices to filter out the threats.

Cheriton discloses propagating filters to an upstream device comprises generating a filter at a first network device where a computer program product for generating filters based on analyzed network flows generally comprises code that analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43). Cheriton discloses a filter is inserted into a firewall located between a router and plurality of servers so data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53). The firewall is preferably a packet filtering firewall but may also be a proxy (application) firewall (col.5, lines 20-25). Network device may also be routers and switches (col.3, lines 58-63 and col.5, lines 26-30). Cheriton discloses that once a group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter and therefore, instead of filtering out all data arriving from the identified organization, only destructive packets received from the actual attacker are dropped (col.7, lines 18-24 and 32-65).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Pearson with Cheriton to teach inserting the filter in a network device such as a firewall because analyzes harmful network flows to prevent network flows from passing through the network device (col.2, lines 29-43)

and data incoming is filtered to reduce the possibility of problems in the network (col.3, lines 38-53). [8]

The alleged combination of Pearson with Cheriton fails to describe or suggest a communication process that communicates statistics collected in the gateway by the monitoring process to a control center and that receives queries or instructions from the control center. The examiner contends that Pearson discloses this feature by: "**a communication process that communicate statistics collected in the gateway from the monitoring process (col.8, lines 10-15 and col. 19, lines 45-50) with a control center and that receives queries or instructions from the control center; (col.7, lines 55-62; col.9, lines 11-17; FIG.1 (controller 112).**" Appellant disagrees. Pearson discloses a conventional intrusion detection mechanism.[9] Cheriton also fails to disclose this feature.[10] Neither of these disclosed mechanisms however correspond to an arrangement by which a gateway collects statistical information pertaining to network traffic and receives queries from a control center to communication the statistics to the control center.

The examiner relies on Pearson's RMC as the control center, arguing that: "... **receives queries or instructions from the control center; (col.7, lines 55-62; col.9, lines 11-17; FIG.1 (controller 112); and col.20, lines 40-50; Pearson discloses the remoter monitoring center (RMC) 130 comprises several components that provide functionality for carrying out various tasks (col.6, lines 42-55). The RMC is the claimed control center where the**

---

[8] Office Action pages 6-8.

[9] Pearson at Col 8, lines 10-45, reproduced below:

In addition to firewall functionality, the preferred communication device 106 implements intrusion detection functionality via intrusion detector 160, by monitoring the communications received into communication device 106 and determining whether such communications comprise an attack or other security risk. More particularly, intrusion detector 160 inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list 170 of known attack signatures. Attack signatures are activity patterns indicative of undesirable activity, i.e., evidence that an unauthorized communication has been received. Examples of attacks include Denial of Service (DoS) attacks, unauthorized access attacks, attempts to modify data or kill programs, protocol violations, and repeated access attempts indicating malicious intent. Representative examples of attack signatures are shown in FIG. 9 and will be further described below with reference to that figure. Intrusion detector 160 may also monitor for attacks by users that are authorized to be on LAN 104. Therefore, any attack or unauthorized activity on the network can be detected and the RMC 130 is automatically notified by an alert signal transmitted by the RMC communications module 165.

The function of intrusion detection is well known to those skilled in the art. Typically, an intrusion detection function is carried out in software, and can be implemented in software, hardwire, or firmware. Typically, intrusion detection is carried out by comparing an incoming communication (usually comprising a string of characters embedded within a TCP/IP packet, such characters being provided by another computer or a user of another computer that is requesting services) to a list of known attack signatures stored in an attack signature list 170. The attack signature list is preferably stored in a rewritable memory within the communication device 106 so that the list can be updated as new attack signatures are identified

[10] Cheriton at Col. 7, lines 33-34, mentions statistics. However, that mention of statistics is based on statistics associated with the aggregate filters.

communication device carries out communications from the RMC (col. 15, lines 52-65 and col. 16, lines 26-29)."[1]

Appellant again disagrees. With respect to the "RMC" Pearson teaches that the RMC receives alert signals from a supported communication device. According to Pearson:

> **The following actions are exemplary of the manner in which the RMC 130 handles an alert signal received from a supported communication device 106. The monitoring engine 114 associated with the RMC 130 receives the alert signal from communication device 106 and forwards the alert, as represented by dashed arrow 156, to selected one of the plurality of remote agents 126a, 126b, . . . 126n. Monitoring engine 114 preferably also maintains a history of attacks on communication device 106 by recording incoming alert signals in a threat database 124 stored in the database farm.**

At col.7, lines 55-62 Pearson discloses that the RMC receives a message or signal indicative of an attack, whereas at col.9, lines 11-17 Pearson discusses attack signatures. Similarly, in FIG.1 (controller 112), Pearson discloses that 112 receives activation and configuration information. While Pearson also discloses that the monitoring engine computer 114 receives threat communications in the form of alert signals from threaten or attacked communication devices, Pearson neither describes nor suggests "a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center." In essence, Pearson neither describes nor suggests that the control center queries the gateway for the statistical information.

The examiner's reliance on teachings from Pearson, directed to the alert signals, is misplaced. The alert signals result from attack signature analysis that determines that an alert should be raised. In contrast, claim 1 by its very terms is directed to communicating statistics collected in the gateway to the control center as part of an analysis that may be conducted by the control center to detect an attack. Thereafter, the control center and or the gateway can raise alerts, etc., as in Pearson, but that raising of alerts is a recited feature of this claim.

In contrast, Cheriton is directed to a stand-alone arrangement, as depicted in Fig. 2. Cheriton neither describes nor suggests a control center and a gateway that receives queries or instructions from the control center. Moreover, Cheriton would have no need to receive queries

---

[1] Office Acton page 7.

or instructions from the control center. Indeed, Cheriton neither has a need for nor does Cheriton possess any equivalent to the recited control center.

Therefore, it is clear that Cheriton does not cure any of the deficiencies in the teachings of Pearson because nowhere does Cheriton disclose to query a gateway from a control center for statistical information on network flows.

Claim 1 also requires a filtering process to insert filters on network devices to filter out packets that the gateway or the control center deems to be part of an attack. Pearson does not teach to insert filters, as generally acknowledged by the examiner.[12] However, in Pearson, (whether at col. 9, lines 11-16, col. 16, lines 36-53, or elsewhere) the occurrence of a match between a detected signature and one stored in the database raises an event, not a filter. Therefore, Pearson fails to teach the "gateway device comprises… a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack."

Appellant notes that the examiner acknowledges this and relies on Cheriton. However, while Cheriton clearly discloses filters, Cheriton does not cure the underlying deficiency in Pearson. Therefore, it is immaterial to patentability whether or nor the combination of Pearson and Cheriton teach the feature of inserting filters, since the remaining features of claim 1, clearly are neither described nor suggested by any combination of Pearson in view of Cheriton.

Claims 29 and 30

For the purposes of this appeal only, claims 29 and 30 stand or fall together. Claim 29 is representative of this group of claims.

Claim 29 is directed to a computer program product … for protecting a victim site during a denial of service attack. Claim 29 includes instructions … to monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic, communicate statistics collected in the computer device to a control center and filter out packets that the device or control center deems to be part of an attack.

[12] Note however the examiner does argue that: "Pearson seems to suggest the claimed a filtering process to filter out packets by an intrusion detector and that all communications are analyzed and compared to the list of known attacks (col.9, lines 11-16 and col. 16, lines 36-53)." Id. page 8.

Pearson, in combination with Cheriton, neither describes nor suggests these features, for analogous reasons as those given in the Appellant's arguments for claim 1. Pearson fails to describe or suggest instructions to communicate statistics collected in the computer device to a control center. Rather, Pearson discloses "attack signatures." In addition, claim 29 includes the feature of "… measure heuristics of the network traffic to provide statistics on the network traffic … ."

The examiner argues that: "**(col.6, lines 6- 19; Pearson discloses a communication device 106 is also referring to a gateway, firewall, or other devices that communicates data between one or more ports. The firewall and intrusion detection functionality of communication device protects the resources of LAN from potential hackers. Thus, the claimed gateway will hereinafter refers to the communication device 106.)**."[13] Appellant contends that this argument is not directed to the claimed feature, namely: "measure heuristics of the network traffic to provide statistics on the network traffic." The examiner appears to be preoccupied with communication but does not address that the feature is "monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic; communicate statistics collected in the computer device to a control center … ."

While it is clear that Pearson combined with Cheriton does not suggest the claimed feature of "monitor … and measure heuristics of the network traffic to provide statistics on the network traffic … ," it is equally clear that Pearson combined with Cheriton does not describe: "instructions to communicate statistics collected in the computer device to a control center.", as discussed above for claim 1.

Appellant contends therefore that assuming *arguendo* motivation to combine, which Appellant does not concede, Pearson combined with Cheriton fails to provide a prima facie case of obviousness because no combination of these references suggests "monitor … and measure heuristics of the network traffic to provide statistics on the network traffic and communicate statistics collected in the computer device to a control center."

Claims 2 and 17

For the purposes of this appeal only, claims 2 and 17 stand or fall together. Claim 2 is representative of this group of claims.

---

[13] Id.

Claim 2 further limits claim 1, and recites that: "the communication process couples to a dedicated link to communicate with the control center over a hardened network." This feature is not described by any combination of Pearson and Cheriton. The examiner contends that: "**See Pearson on col.3, lines 59-65 and col. 12, lines 30-33; discussing the communication process couples to a dedicated link to communicate with the control center over a hardened network.**." [14]

The examiner relies on the teaching in Pearson that on waking up, the system sends a wake-up signal on an encrypted channel.[15] However, that is not what is claimed by Appellant. Rather, Appellant claims that the there is "a dedicated link to communicate with the control center over a hardened network." The encrypted channel is not a dedicated link and moreover it appears that the process occurs at activation, and is not carrying the network traffic of base claim 1 to the control center. There is no mention in Pearson that the network that the communication process uses to communicate with the control center is a dedicated. Rather, it appears to be the same network that is monitored by the "communications device."

Claims 5, 20 and 31

For the purposes of this appeal only, claims 5, 20 and 31 stand or fall together. Claim 5 is representative of this group of claims.

Claim 5 further limits claim 1 requiring that the gateway is adaptable to dynamically install the filters on nearby routers. The examiner argues that: "See Cheriton on col.2, lines 50-63 and col.5, lines 26-30; discussing the gateway is adaptable to dynamically install filters on nearby routers."[16]

Cheriton discloses: "The system further includes a filter generator operable to generate a filter to prevent packets corresponding to the identified potentially harmful network flows from passing through the network device."[17] Appellant contends that Cheriton's discussion regarding a filter generator however does not meet the claimed element that the "gateway is adaptable to dynamically install filters on nearby routers. Cheriton does not disclose that the gateway installs filters on routers. Rather, Cheriton teaches away from this feature by:

---

[14] Id. page 9.
[15] See Pearson col. 3, lines 59-65 and col. 12, lines 30-33.
[16] Office Action page 9.
[17] Cheriton col. 2, lines 50-54.

> The system is used to detect harmful network flows which may include denial of service attacks or merely a high rate of data coming into the system which needs to be filtered to reduce the possibility of problems within the network. As described below, the system may also use an inter-router filter propagation protocol (FPP) to automatically propagate filter information upstream to filter data closer to the source of the data, as illustrated by filter 22 located at router 14. [18]

While Cheriton does mention a filter, and does show a filter on the router and the firewall associated with the computer device of Fig. 2, Cheriton does not describe any mechanism that would permit filters installed by the gateway on nearby routers. Appellant contends that it would not be obvious from any combination of Pearson with Cheriton to install filters on nearby routers since Cheriton is not directed to a distributed approach and Pearson neither suggests deployment of filters on routers nor the underlying statistical information by which the filters are generated.

Claims 6, 8, 9, 21, 23, 24, 32, 34 and 35

For the purposes of this appeal only, claims 6, 8, 9, 21, 23, 24, 32, 34 and 35 stand or fall together. Claim 6 is representative of this group of claims.

Claim 6 further limits claim 1 by reciting that: "the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets." The examiner relies on col. 13, lines 4-29 and col. 15, lines 30-33; of Pearson for this feature. Claim 8 recites that the monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports, whereas claim 9 recites that the monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

Claim 6 will be used to argue why Pearson combined with Cheriton fails disclose the features of any of these claims. The examiner argues: "**See Pearson on col. 18, lines 51-67; discussing the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.**"

At that passage (**col. 18, lines 51-67**) Pearson describes:

---

[18] Id. at col. 3, lines 48-54.

> **Each exemplary entry on the list 170 comprises a header field 810, a body field 820, and a two-bit priority field 826. The priority field 826 in the disclosed embodiment is 00=ignore, 01=low priority, 10=not assigned (unused), and 11=high priority. Those skilled in the art will understand that the priority field is set in accordance with user and/or predetermined remote monitoring system preferences, for example by establishing certain predetermined priorities for certain types of signatures via a high, medium, or low set policy (FIG. 4A), or by user setting of priority through the advanced options settings (FIG. 4B).**

Pearson is not referring to statistical information pertaining to any of the features of claim 6. Rather, Pearson disclosed the composition of an entry in the list of attack signatures. Attack signatures are not statistical information pertaining to packet flows, but instead portions of the packet, e.g., payload and/or header. In any event, the entries described at that passage in Pearson neither describe nor suggest: "levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets."

Similarly, Pearson combined with Cheriton fails to disclose at the cited passages or elsewhere that "the monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports," as in claim 8 or that "the monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection," as in claim 9.

Claims 7, 22, 33

For the purposes of this appeal only, claims 7, 22, and 33 stand or fall together. Claim 7 is representative of this group of claims.

Claim 7 further limits the gateway of claim 1 by reciting that the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses. The examiner argues for claim 7 that: "**See Pearson on col. 17, lines 35-47 and Cheriton on col.8, lines 1-44; discussing the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.**"

Pearson at the cited passages discusses threat events and priority of such events. Nowhere however does Pearson discuss "determines levels of IP packets that have bad source

addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses."

Cheriton, meanwhile discusses the aggregate filters and use of ICMP packets. Specifically, the Cheriton discloses:

> **The flow analyzer 122 monitors the statistics associated with these aggregate filters 10. If the statistics associated with an aggregate filter entry indicate a potential problem (or just as a periodic check of the traffic distribution), creation of netflow entries is enabled for packets matching this entry. Consequently, the flow analyzer 122 receives a flow record 120 for each flow matching this aggregate. Using this specific flow information, the flow generator 124 determines how to refine the aggregate filter. For example, the flow label information may indicate that most ICMP packets are coming from a particular source address. In this case, the flow generator 124 can configure an aggregate filter 10 that matches ICMP packets from that source, establishing a separate policer for that filter or potentially just blocking the source. The original aggregate filter is preferably retained as well so that all other ICMP traffic matches to this original filter. The flow analyzer 122 can then monitor the statistics of the original aggregate filter with the offending host removed, to detect whether there are further anomalies within the aggregate flow.**[19]

Thus, according to Cheriton, the flow analyzer receives a flow record for each flow and uses, e.g., ICMP packets from a particular address to indicate source of an attack. Nonetheless, claim 7 specifically recites to "determine levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses." Therefore, the purported combination of Pearson and Cheriton whether at the cited passages or elsewhere neither describes nor suggests these features.

Claims 10, 25 and 36

For the purposes of this appeal only, claims 10, 25, and 36 stand or fall together. Claim 25 is representative of this group of claims.

Claim 25 limits claim 16, and recites that monitoring comprises "detecting sustained rate higher than plausible for a human user over a persistent HTTP connection." The examiner contends that: "**As per claim 10: See Pearson on col. 10, lines 33-38 and Cheriton on col. 8, lines 30-44; discussing monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection.**" At col. 10, lines 33-38, Pearson discusses user changing a security policy of a network, which

[19] Cheriton Col. 7, line 58 to Col. 8, line 10.

has no relevance to the claimed feature. Cheriton at col. 8, lines 30-44 discusses configurations to the system that may also be used "**to automatically recognize further structure to network traffic that does not necessarily represent an attack or a failure.**" Cheriton uses a search engine spider as an example where Cheriton would automatically detect a high demand source of this nature, and the filter generators would automatically reconfigure the filters to handle this demand.. However these teachings in Cheriton also do not address the claimed feature.

Cheriton also discusses that "**the system can be used to identify sources that appear to represent excessive traffic, allowing aggregate filters to be created that separate them out of the overall aggregate and throttle their traffic appropriately. These filters 10 can also be automatically removed when the associated traffic drops off, based on the statistics associated with the identified flow. Thus, for example, once a search engine finishes its searching at a web site, the filter 10 created for it indicates that traffic has dropped because of the lower rate and the specific filter can be reclaimed.**" However, this again is in the context of throttling the aggregate filter and is not part of the monitoring that produces statistics (sustained rate higher than plausible for a human user over a persistent HTTP connection of claim 7) used for filtering out packets that the gateway or control center deems to be part of an attack.

Claim 11

Claim 11, which recites that the "monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail," is neither described nor suggested by Pearson combined with Cheriton. The examiner relies on Pearson col. 11, lines 8-12 and Cheriton col.7, lines 32-65 for this feature. In the cited passage from Pearson, the reference discusses user selecting security policies, not maintaining statistical summary information on traffic over different periods of time.

Cheriton col.7, lines 32-65 are reproduced below:

> **The initial class of packets 78 to be analyzed is selected based on statistics associated with the aggregate filters, as described below. The data which is to be analyzed is periodically changed or updated to further refine a filter once it has been generated. For example, a first class of packets 78 may be analyzed for 0.5 second then a next class of packets analyzed for the next 0.5 seconds. The initial filters 10 may be configured according to user specified configurations or default values. The flow analyzer 122 and filter generator 124 then use the analyzed flow to determine if the existing filters need to be refined or new filters need to be generated. Based on the analyzed flow, the filter generator 124 will tell (or modify) the ACL classifier 80, which then affects the netflow entries that are created. The**

> **class of packets 78 selected may be based on a class of packets which have been identified as potentially harmful, or may be randomly chosen. The ACL classifier 80 may, for example, begin by looking at flows 64 for all packets 78 received from a source with an IP address having the form 3.xxx.xxx.xxx, where xxx represents any possible value from zero to 255. If a problem is identified in one of the packets streams 64, the ACL classifier 80 may be then instructed to look at flows for all packets 78 received from a source having an IP address of 3.141.xxx.xxx. This may be narrowed down further to refine the filter 10.**
>
> **The flow analyzer 122 monitors the statistics associated with these aggregate filters 10. If the statistics associated with an aggregate filter entry indicate a potential problem (or just as a periodic check of the traffic distribution), creation of netflow entries is enabled for packets matching this entry. Consequently, the flow analyzer 122 receives a flow record 120 for each flow matching this aggregate. Using this specific flow information, the flow generator 124 determines how to refine the aggregate filter. For example, the flow label information may indicate that most ICMP packets are coming from a particular source address. In this case, the flow generator 124 can configure an aggregate filter 10 that matches ICMP packets from that source, establishing a separate policer for that filter or potentially just blocking the source. The original aggregate filter is preferably retained as well so that all other ICMP traffic matches to this original filter. The flow analyzer 122 can then monitor the statistics of the original aggregate filter with the offending host removed, to detect whether there are further anomalies within the aggregate flow.**

Claim 11 is neither described nor suggested by these teachings whether taken separately or in combination with Pearson or any other teaching in Cheriton. Claim 11 calls for "monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail." Nowhere does Cheriton teach to maintain statistical information or a summary of the information over different periods of time and different levels of detail. Cheriton teaches: "**The data which is to be analyzed is periodically changed or updated to further refine a filter once it has been generated. For example, a first class of packets 78 may be analyzed for 0.5 second then a next class of packets analyzed for the next 0.5 seconds.**" Cheriton thus discloses to change data to be analyzed, e.g., to refine the filters and monitor different classes of packets. However, Cheriton does not teach "monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail.", as called for in claim 11.

Claims 12, 26 and 37

For the purposes of this appeal only, claims 12, 26 and 37 stand or fall together. Claim 12 is representative of this group of claims.

Claim 12 sets forth some of the parameters for which statistical information is provided by the monitoring process. Claim 12 recites: "statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections

or of packets sent in either direction." No combination of Pearson and Cheriton either describes or suggests maintaining statistical information on these specific parameters.

The examiner relies on "Cheriton on col.5, lines 20-25 and col.7, lines 32- col.8, line 10." However, at these passages and elsewhere Cheriton does not describe the claimed features. Cheriton at col.5, lines 20-25 discusses to allow specific source addresses to access specific destination addresses and at 7, lines 32- col.8, line 10 discusses statistics of the aggregate filters, but does not mention maintaining statistics on these specific parameters.

Claims 13, 27 and 38

For the purposes of this appeal only, claims 13, 27 and 38 stand or fall together. Claim 13 is representative of this group of claims.

Claim 13 recites that the "monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold." The examiner relies on Pearson col.8, lines 10-32 and col. 17, lines 1-10 for this feature. However, at col. 8, lines 10-32 Pearson discusses intrusion detection and attack signatures, not measured parameters, whereas at col. 17, lines 1-10, Pearson discusses different event threat levels. Pearson does not compare measured parameters to thresholds at those passages. Thus, neither at those passages nor elsewhere does Pearson suggest the "monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold."

Claim 15

Claim 15 recites that the: "monitoring process logs specific packets identified as part of an attack to enable an administrator to identify important properties of the attack." This feature directed to examining of specific packets further distinguishes over the cited art since it requires both the monitoring to produce statistical information on network flows and examination of specific packets.

Claim 39

Claim 39 distinguishes over the combination of Pearson with Cheriton, since the combination neither describes nor suggests "… instructions to cause the processor to receive communications from a control center to deliver data pertaining to the types of traffic passing through the gateway."[20] Neither Pearson non Cheriton taken in any combination suggests the feature of "receive communications from a control center to deliver data," as generally discussed above.

Conclusion

Appellant submits, therefore, that Claims 1-39 are neither described by nor obvious over any purported combination of Pearson in view of Cheriton and are otherwise allowable over the cited art. Therefore, the Examiner erred in rejecting Appellant's claims and should be reversed.

Respectfully submitted,

Date: 9/29/10

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21767669.doc

[20] In claim 39 there is not antecedent basis for "processor" and "gateway," but functionally those are equivalent to the "computing device" recited in base claim 29. Appellant will amend this claim after the Board's decision.

Appendix of Claims

1. A gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises:

a computing device comprising:

a monitoring process that monitors network traffic through the gateway;

a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center; and

a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack.

2. The gateway of claim 1 wherein the communication process couples to a dedicated link to communicate with the control center over a hardened network.

3. The gateway of claim 1 wherein the monitoring process in the gateway samples network packet flow in the network.

4. The gateway of claim 1 wherein the gateway is adaptable to be physically deployed in line in the network.

5. The gateway of claim 1 wherein, the gateway is adaptable to dynamically install the filters on nearby routers.

6. The gateway of claim 1 wherein the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

7. The gateway of claim 1 wherein the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

8. The gateway of claim 1 wherein monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports.

9. The gateway of claim 1 wherein monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

10. The gateway of claim 1 wherein monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection.

11. The gateway of claim 1 wherein monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail.

12. The gateway of claim 11 wherein monitoring process maintains statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

13. The gateway of claim 12 wherein monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold.

14. The gateway of claim 13 wherein monitoring process logs packets.

15. The gateway of claim 14 wherein monitoring process logs specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

16. A method of protecting a victim site during a denial of service attack, comprises:

disposing a gateway device between the victim site and a network;

monitoring network traffic through the gateway and measuring heuristics of the network traffic to provide statistics network traffic;

communicating the statistics collected in the gateway to a control center; and

filtering out packets that the gateway or control center deems to be part of an attack.

17. The method of claim 16 wherein communicating occurs over a dedicated link to the control center via a hardened network.

18. The method of claim 16 wherein monitoring samples network packet flow in the network.

19. The method of claim 16 wherein the gateway is physically deployed in line in the network.

20. The method of claim 16 wherein filtering further comprises:

dynamically installing filters on nearby routers via an out of band connection.

21. The method of claim 16 wherein monitoring further comprises:

detecting IP traffic and determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

22. The method of claim 16 wherein monitoring further comprises:

detecting Internet Protocol (IP) traffic and determining levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

23. The method of claim 16 wherein monitoring further comprises:

detecting Internet Protocol (IP) traffic and determining levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

24. The method of claim 16 wherein monitoring further comprises:

detecting IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

25. The method of claim 16 wherein monitoring further comprises:

detecting a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

26. The method of claim 16 wherein monitoring further comprises:

logging statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

27. The method of claim 16 wherein monitoring further comprises:

issuing a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

28. The method of claim 16 wherein monitoring further comprises:

logging specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

29. A computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises instructions for causing a computer device coupled at an entry to the site to:

monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic;

communicate statistics collected in the computer device to a control center; and

filter out packets that the device or control center deems to be part of an attack.

30. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

sample network traffic flow.

31. The computer program product of claim 29 wherein instructions to filter further comprise instructions to:

dynamically install filters on nearby routers via an out of band connection.

32. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect IP traffic; and

determine levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

33. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect Internet Protocol (IP) traffic; and

determine levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

34. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect Internet Protocol (IP) traffic; and

determine levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

35. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

detect IP traffic; and

determine levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

36. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

detect a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

37. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

log statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

38. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

issue a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

39. The computer program of claim 29 further comprising instructions to cause the processor to receive communications from a control center to deliver data pertaining to the types

of traffic passing through the gateway.

Evidence Appendix

None

Related Proceedings Appendix

None